Listing of Claims

1. (Previously Presented) A method for securing contents of one or more data storage devices within a computer capable of storing a security password for unlocking and locking the data storage devices and of supporting one or more security features, the method comprising:

reading from each of the data storage devices within the computer one or more data storage device identifiers;

determining from the data storage device identifiers whether the data storage device supports the security features and is locked;

in response to determining that the data storage device supports the security features and is locked, determining whether the data storage device is returning from a powered off state or a hardware reset;

in response to determining that the data storage device is locked and returning from a powered off state or a hardware reset, receiving from a user a password for unlocking the data storage device;

in response to receiving the password, determining whether the received password is the security password; and

in response to the received password being the security password, unlocking the data storage device and thereby allowing access to data stored on the data storage device.

2. (Previously Presented) The method of claim 1, wherein the method is implemented during a power on test procedure of the computer hosting the data storage devices.

3. (Previously Presented) The method of claim 1, further comprising:

in response to the received password not being the security password, determining whether limited access should be provided to each locked data storage device;

in response to determining that limited access should be provided, setting a bit corresponding to each locked data storage device to exclude the locked data storage device from detection verification during a power on test procedure; and

in response to determining that limited access should not be provided to each locked data storage device, isolating each locked data storage device from the operating system.

4. (Original) The method of claim 3, wherein limited access comprises prohibiting reading from or writing to the locked data storage device.

5. (Original) The method of claim 1, wherein the data storage devices are locked upon experiencing a powered off state, a sleep state, or a hardware reset, and wherein the method further comprises:

in response to the received password being the security password, determining whether a data storage device returning from a sleep state should be unlocked without requiring a user to enter a password; and

in response to determining that the data storage device should be unlocked without requiring a user to enter a password, storing the security password within a memory located outside the data storage device.

6. (Original) The method of claim 5, further comprising:

in response to determining that the data storage device is locked, determining whether the data storage device is returning from a powered off sleep state;

in response to the data storage device being locked and returning from a powered off sleep state, determining whether the data storage device was unlocked prior to the sleep state;

in response to determining that the data storage device was unlocked prior to the sleep state, determining whether a data storage device returning from a sleep state should be unlocked without requiring a user to enter a password; and

in response to determining that the data storage device should be unlocked without requiring a user to enter a password, retrieving the security password from the memory and utilizing the security password to unlock the data storage device.

7. (Original) The method of claim 6, wherein the security password is stored within the memory in an encrypted format.

8. (Original) The method of claim 6, further comprising in response to determining that the data storage device should be unlocked after returning from a sleep state by requiring a user to enter a password, receiving the security password from a user and utilizing the security password to unlock the data storage device.

9. (Original) The method of claim 1, further comprising:

in response to determining that the data storage device is unlocked, determining whether a security password has been enabled; and

in response to determining that the data storage device is unlocked and that no security password is enabled for the data storage device, disabling, until a next power cycle, the security features that enable security passwords.

10. (Original) The method of claim 1, further comprising:

in response to the data storage device being locked and returning from a powered off state or a hardware reset, determining whether a backup password may be used to unlock the data storage device;

in response to determining that a backup password may be used, determining whether a request to enter a backup password has been received;

in response to receiving a request to enter a backup password, receiving from a user a password for unlocking the data storage device; and

in response to the received password being the backup password, unlocking the data storage device and thereby allowing access to data stored on the data storage device.

11. (Original) The method of claim 10, further comprising:

in response to the received password being the backup password, determining whether a maximum security is supported by the security features; and

in response to the received password being the backup password and the maximum security being supported, erasing the data storage device before unlocking the data storage device.

12. (Original) The method of claim 1, wherein a password entry attempt counter is set for a maximum number of entry attempts allowed, further comprising:

in response to determining that the password is not the security password, determining whether the password entry attempt counter is equal to zero;

in response to the password entry attempt counter being greater than zero, decrementing the password entry attempt counter by one and again receiving a password from a user; and

in response to the password entry attempt counter equaling zero, prohibiting additional password entries until a next power cycle and displaying a message that the data storage device remains locked.

13. (Original) The method of claim 1, further comprising executing a setup utility within the basic input/output system operative to control one or more functions for manipulating at least one of a security password and a backup password for a data storage device supporting the security features wherein the functions are accessed by one of entering the security password when prompted by the setup utility and selecting the data storage device in the setup utility when said data storage device is unlocked.

14. (Original) A computer-controlled apparatus capable of performing the method of Claim 1.

15. (Original) A computer-readable medium comprising computer executable instructions which, when executed by a computer, cause the computer to perform the method of Claim 1.

16. (Previously Presented) A system for securing the contents of one or more data storage devices capable of storing a security password for unlocking and locking the data storage devices located within a computer, the system comprising:

a memory;

a basic input/output system (BIOS) stored within the memory for controlling the basic input/output functions of the computer, wherein the BIOS comprises a BIOS security setup utility that is operative during a BIOS runtime to control functions for manipulating data storage

device security, and wherein the BIOS security setup utility is independent from an operating system of the computer; and

a central processing unit operative to execute the BIOS stored in the memory.

17. (Previously Presented) The system of claim 16, wherein the BIOS setup utility is operative to receive a selection of a data storage device, receive a selection of a password function to perform on the selected data storage device, determine whether a security password has been enabled for a selected data storage device, in response to the security password not being enabled, receive from a user a security password, and in response to receiving the security password from the user, enable the security password on the selected data storage device, wherein enabling the security password includes storing the security password on the selected data storage device thereby preventing access to contents of the selected data storage device when the selected data storage device is locked with the security password.

18. (Previously Presented) The system of claim 17, wherein the BIOS setup utility is further operative to determine whether a hardware reset is performed when the BIOS setup utility is exited and in response to determining that a hardware reset is not performed when the BIOS setup utility is exited, exit the BIOS setup utility and remove power from the selected data storage device thereby locking the selected data storage device with the security password.

19. (Previously Presented) The system of claim 17, wherein the BIOS setup utility is further operative to one of:

in response to the security password being enabled, receive a password from a user, in response to receiving a password, determine whether the password is the security password by attempting to disable security for the selected data storage device with the password, and in response to the received password being the security password, disable then re-enable the security of the selected data storage device thereby validating the password as the security password; and

in response to the security password being enabled and the data storage device being unlocked, grant access to the functions for manipulating data storage device security.

20. (Previously Presented) A method of securing the contents of a data storage device within a computer wherein the data storage devices are locked upon experiencing a sleep state, the method comprising:

storing a security password within a memory located within the computer, but outside the data storage device;

in response to determining that the data storage device is locked, determining whether the data storage device is returning from a sleep state;

in response to the data storage device being locked and returning from a sleep state, determining whether the data storage device was unlocked prior to the sleep state; and

in response to determining that the data storage device was unlocked prior to the sleep state, retrieving the security password from the memory and utilizing the security password to unlock the data storage device.

21. (Original) The method of claim 20, wherein the security password is stored within the memory in an encrypted format.